REMARKS/ARGUMENTS

Claims 1-68 are pending. No claim is amended.

The Examiner has not acknowledged the IDSs that were filed September 16, 2004 and June 14, 2005. Applicants respectfully request acknowledgment of the above-mentioned IDSs by initialing and returning the attached copies of the same IDSs.

Claims 1-68 are rejected under 35 U.S.C.§ 102(e) as being anticipated by Lewis (US 6,233,565). However, other than citing long sections of Lewis (e.g., col. 8, line 8 to col. 12, line 42), the Examiner has not pointed out which specific sections of Lewis that teach each of the limitations in the rejected claims, for example, claim 1.

MPEP 707.07(d) states that "[a]n omnibus rejection of the claim 'on the references and for the reasons of record' is stereotyped and usually not informative and should therefore be avoided." However, the Examiner rejects all the pending claims over Lewis reference in an omnibus and general manner and without mentioning any specific text, other than, a large and broad portion of Lewis ("figs 1-3, col. 6, line 49 to col. 7, line 35; col. 8, line 8 to col. 12, line 42) applied to all limitations of claim 1, as a group. See, Office action, page 3, first paragraph.

Nevertheless, Applicants respectfully submit that Lewis does not teach the claimed invention.

Independent claim 1 includes, among other limitations, "a plurality of cryptographic devices remote from the plurality of user terminals and coupled to the computer network," "wherein each cryptographic device is capable of performing value management functions for one or more users," "wherein each cryptographic device is not dedicated to particular user terminals," and "wherein each cryptographic module is programmable to service any of the plurality of user terminals."

First, in regard to the element of "a plurality of cryptographic devices remote from the plurality of user terminals," the system of Lewis dose not have a plurality of cryptographic devices remote from the plurality of user terminals. Rather, Lewis describes a single cryptographic module (14) that is remote from the users. As illustrated in FIG. 1, Lewis

discloses a remote service provider (RSP) 4, and a third party seller of goods and/or services (TPS) 6... . The client 2n has a Host system 10n and a PSD 20n which is resident on a [single] server of RSP 4. The Host 10n accesses the remote PSD 20n via the Internet 30." (Col. 6. lines 39-59, emphasis added). The single server 4 comprises of its own single cryptographic module 14. (Col. 21, lines 64-65, emphasis added). Lewis further describes that each client 2n has its own cryptographic module 12. However, these client cryptographic modules 12 are not each "remote from the plurality of user terminals." That is, at least one of the client cryptographic modules 12 is local to at least one user terminal.

Second, regarding the element of "wherein each cryptographic device is capable of performing value management functions for one or more users," Lewis does not teach this element. Rather, in the system of Lewis, a Transaction Manager server 180 performs value management functions for all of the users. See, for example, Col. 25, lines 5 -1, emphasizing that "once the client 2 has been authenticated, it submits a transaction request to the transaction server 180 and waits for a response. It now becomes the job of the Transaction Manager to process the transaction and return a "receipt" to the client 2. All transaction "receipts" will contain a date/time stamp, and a sequence number and a digital signature to verify the authenticity of a transaction . . .." Therefore, "processing value" in Lewis is performed by the transaction server 180 and not by each of a plurality of cryptographic devices.

Third, regarding the element of "wherein each cryptographic device is not dedicated to particular user terminals," Lewis does not teach this element. As explained above, at least one of the client cryptographic modules 12 of Lewis is local to at least one user terminal. Therefore, that local cryptographic module is dedicated to particular user terminal.

Fourth, regarding the claimed element "wherein each cryptographic module is programmable to service any of the plurality of user terminals.," Lewis fails to teach this element. First, as mentioned above, the system of Lewis dose not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a plurality of server cryptographic devices remote from the plurality of users, there is no description in Lewis that each of these imaginary server cryptographic devices is capable of

servicing any of the plurality of remote users. In fact, Lewis specifically describes that the cryptographic module 14 stores the Client Public Authentication Keys, which are used to prove the client's identity (that is, to authenticate the client), when a client attempts to establish a connection with the server 4. (Col 25, line 63-67. Also, see, Table III at the end of Col. 27, and col. 27, lines 58-59.).

Therefore, even if Lewis had a plurality of server cryptographic devices remote from the users, each of those devices would not have been able to service (e.g., authenticate) any of the plurality of users, because each cryptographic device would have had to maintain and update the Public Authentication Keys for all of the clients. There is no teaching in Lewis about this. Furthermore, each of the imaginary server cryptographic devices of Lewis would have had to be "stateless device, meaning that a PSD package can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package." (Specification, page 8, lines 13-16). Moreover, a PSD package for each of the imaginary server cryptographic devices would have had to include "all data needed to restore the PSD to its last known state when it is next loaded into a [different] cryptographic module." (Id., lines 22-24). There is no teaching in Lewis about this either.

Indeed, Lewis specifically describes that the cryptographic module 14 maintains the Client Private Indicium Keys, which are used to generating indicia data for that client. (Table III at the beginning of col. 28). Therefore, even if Lewis had a plurality of server cryptographic devices remote from the users, each of those devices would not have been able to, for example, generate indicia data for transmitting to any of the plurality of users, because each cryptographic device would have had to maintain and update the Client Private Indicium Keys for all of the clients. There is no disclosure in Lewis about this.

Moreover, Lewis describes that "the first step to indicium generation is generating a public/private key pair for the server 4 [cryptographic module 14]. The public key is sent to the Certification Authority and a certificate for that server 4 is generated and returned to the Server. The Certification Authority also retains this certificate so that the Certification Authority can verify the authenticity of future server requests. Similarly, the server 4 will have a copy of the

CA's certificate to verify the authenticity of data being sent back from the CA." (Col. 30, line 63 to col. 31, line 4). Consequently, the Certification Authority would have had to retain a different certificate for each of the imaginary server cryptographic devices to service any of the user terminal, for example, verify the authenticity of future server requests. There is no teaching in Lewis about this either.

Fifth, each of the imaginary server cryptographic devices of Lewis would have had to be "stateless device and a PSD package for each of the imaginary server cryptographic devices would have had to include "all data needed to restore the PSD to its last known state when it is next loaded into a [different] cryptographic module." (Specification, page 8, lines 13-24). There is no teaching in Lewis about this either.

In short, based on at least the above-mentioned **five arguments**, the independent claim 1 is not anticipated by Lewis.

Independent claim 30 includes, among other limitations, "securing the information about the users in the database by one or more of cryptographic devices from a plurality of cryptographic devices remote from the plurality of user terminals," performing value management functions in the one or more of the cryptographic devices for one or more of the plurality of users," "wherein the cryptographic device is not dedicated to specific user terminals," and "wherein each of the plurality of cryptographic devices accesses data elements for any of the plurality of user terminals."

As explained above, Lewis does not teach the above limitations. Therefore, independent claim 30 is not anticipated by Lewis either.

Independent claim 57 includes, among other limitations, "wherein the cryptographic device is not dedicated to particular users on the computer network,: and "wherein the cryptographic device processes data for any of the plurality of users." As described above, Lewis does not teach the above limitations. Consequently, independent claim 57 is not anticipated by Lewis either.

In short, independent claims 1, 30 and 57 are patentable in view of the cited references. Dependent claims 2-29, 31-56 and 58-68 depend from claims 1, 30 and 57, respectively and

include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested. If the Examiner believes that a telephone conference would be useful in moving this application forward to allowance, the Examiner is encouraged to contact the undersigned at (626) 795-9900.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS672760.1-*-03/17/06 1:50 PM